

CLAIMS

What is claimed is:

Sub A
1. A system for monitoring operation of a software program in a network environment, comprising:

an execution component for executing the software program, said execution component being coupled to an isolated network that does not have a direct connection to another network that is not an isolated network;

a monitoring component for obtaining information about actions performed by the software program; and

a network emulation component, coupled to said isolated network, for emulating the behavior of at least a host providing network services; wherein

said execution component and said network emulation component cooperate with said isolated network in order to elicit a behavior of the software program that is detectable by said monitoring component.

2. A system as in claim 1, where said emulation component further comprises a server programmed so as to return emulated results in response to a request resulting from the software program being executed on said execution component.

3. A system as in claim 1, where said emulation component is programmed so as to limit access by the software program to only certain resources.

002780 ESTH01960

4. A system as in claim 1, where at least one of said emulation component and monitoring component are programmed so as to provide information about the performance of the software program for the purposes of testing, debugging, performance profiling, or optimization.

5. A system as in claim 1, where at least one of said emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program.

6. A system as in claim 1, where at least one of said emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of detecting a presence of an undesirable software entity within the software program.

7. A system as in claim 6, wherein the undesirable software entity comprises at least one of a worm or a virus.

8. A system as in claim 6, wherein the undesirable software entity comprises a worm that exhibits viral characteristics.

9. A system as in claim 1, where the elicited behavior of the software program comprises self-replication.

10. A system as in claim 1, where the elicited behavior of the software program comprises viral or malicious activity.

11. A system as in claim 2, where said server is programmed to determine what result to return based at

09640453-081700

13. A system as in claim 2, where said server comprises at least one of a real or an emulated Web server.

15. A system as in claim 2, where said server comprises at least one of a real or an emulated router.

16. A system as in claim 2, where said server comprises at least one of a real or an emulated DNS, WINS, or other Name server.

17. A system as in claim 2, where said server comprises at least one of a real or an emulated SNMP server.

18. A system as in claim 2, where said server comprises at least one of a real or an emulated NetBIOS server.

19. A system as in claim 2, where said server comprises at least one of a real or an emulated server that operates in accordance with SMB, NFS or other distributed file system protocols.

28. A system as in claim 27, wherein said at least one emulated network server operates as an optimistic server when responding to requests received from said emulated

data communications network.

29. A system as in claim 27, wherein the desired behavior is indicative of a presence of an undesirable software entity within the software program.

30. A system as in claim 29, wherein the undesirable software entity comprises at least one of a worm or a virus.

31. A system as in claim 29, wherein the undesirable software entity comprises a worm that exhibits viral characteristics.

32. A system as in claim 27, where the desired behavior comprises self-replication.

33. A system as in claim 27, where the desired behavior comprises viral activity or malicious activity.

34. A system as in claim 27, wherein said monitor operates to detect at least one of a creation of a new file, a receipt of mail, an opening of mail, a posting of news, an opening of a new socket connection, an execution of a particular application, and an alteration of a system registry.

35. A system as in claim 27, where at least one of said emulated host computer and said monitor are programmed so as to provide information about the performance of the software program for the purposes of testing, debugging, performance profiling, or optimization.

36. A system as in claim 27, where at least one of said emulated host computer and said monitor are programmed so as to provide information about the performance of the

002780" E5404960

software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program.

37. A computer program embodied on at least one computer-readable medium for executing a method for eliciting a behavior from a software program, the method comprising steps of:

emulating a data communications network having at least one emulated network server coupled thereto, said at least one emulated network server operating to respond to requests received from said emulated data communications network;

emulating a host computer coupled to said emulated data communications network, said emulated host computer executing the software program, the software program operating to originate requests to said emulated data communications network; and

detecting an occurrence of the behavior in at least one of said emulated network server and said emulated host computer.

38. A computer program as in claim 37, and further comprising a step of emulating at least one goat computer coupled to said emulated data communications network, and wherein the step of detecting an occurrence of the behavior detects the occurrence of the behavior in said at least one goat computer.

39. A computer program as in claim 37, wherein the elicited behavior is indicative of a presence of an undesirable software entity within the software program.

09640453 "081700

46. A computer program as in claim 37, wherein said method provides information about the performance of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program.